

AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1. (Currently Amended) A system configured to arrange end-to-end (e2e) encryption between two or more pieces of terminal equipment communicating with one another, said terminal equipment comprising:
 - a codec configured to convert an audio signal into a dataflow and vice versa,
 - a module configured to manage encryption parameters stored in connection with the terminal equipment,
 - an encryption key stream generator KSG configured to generate a key stream segment (KSS) with the said encryption parameters,
 - a module configured to encrypt a dataflow and decrypt the encryption with the generated key stream segment,
 - a module configured to synchronize the encrypted dataflow and to de-synchronize the synchronization, and
 - at least one interface configured to receive the encryption parameters from the data communication network,and wherein at least one of the pieces of terminal equipment is configured to function as a special server terminal device, ~~to manage and distribute at least the encryption parameters concerning a data communication network to the other pieces of terminal equipment based on an established criterion~~ being configured to manage at least one of encryption and synchronization applications as well the encryption parameters concerning a data communication network and to distribute these based on an established criterion to the other pieces of terminal equipment, and wherein
 - ~~the special server terminal device is configured to manage at least one of encryption and synchronization applications and to distribute these based~~

~~on an established criterion to the other pieces of terminal equipment and~~
the terminal equipment is configured to download said applications from
said special terminal device and to manage said applications, where the
terminal equipment comprises a
data memory configured to store the applications and
a processor and operating memory configured to execute the applications.

2. (Currently Amended) A system according to claim 1, wherein the terminal equipment is configured to run applications of ~~J2ME (Java 2 Platform Micro Edition)~~ a java 2 platform micro edition specification with said processor.

3. (Currently Amended) A system according to claim 2, wherein the terminal equipment is configured in accordance with ~~the MIDP (Mobile Information Device Profile)~~ a mobile information device profile specification.

4. (Currently Amended) A system according to claim 1, wherein the downloading of ~~applications~~ the at least one of encryption and synchronization applications as well as the encryption parameters at the terminal equipment is arranged to take place in a self-organizing manner, ~~such as, for example, as SDS (Short Data Service)~~ with short data service messages.

5. (Currently Amended) An apparatus, comprising:

a module configured to carry out encryption,
one or more modules configured to carry out synchronization,
a module configured to receive and manage at least encryption keys, and
a module configured to download and manage at least one of ~~dynamic~~
encryption and synchronization applications as well as encryption
parameters.

wherein a functionality of the apparatus to carry out end-to-end encrypted communication with another apparatus is implemented by the at least one ~~dynamic application of encryption~~ and synchronization applications as well as the encryption parameters based on a program.

6. (Currently Amended) The apparatus according to claim 5, wherein said application is configured to arrange command functionality at least at an interface between ~~the SIM~~ a subscriber identity module and a terminal equipment through a mobile information device profile application protocol programming interface (~~MIDP API~~) of the application.

7. (Currently Amended) A method, comprising:
receiving from a data communication network information comprising at least one ~~dynamic encryption application~~ of encryption and synchronization applications as well as encryption parameters, and at least one encryption key; and
executing the at least one ~~dynamic encryption application~~ of encryption and synchronization applications as well as the encryption parameters to control the operation of a terminal equipment in order to implement secure end-to-end (~~e2e~~) data communication with another terminal equipment using the at least one encryption key.

8. (Currently Amended) The method of claim 7, where the at least one ~~application~~ of encryption and synchronization applications as well as the encryption parameters, and the at least one encryption key are stored in a subscriber identity (~~SIM~~) module on the terminal equipment, and the ~~application~~ at least one of encryption and synchronization applications is executed to arrange command functionality between the ~~SIM~~ subscriber identity module and the terminal equipment through a programming interface of the application.

9. (Currently Amended) The method of claim 7, wherein receiving the at least one ~~application~~ of encryption and synchronization applications as well as the encryption parameters is arranged to take place in a self-organizing manner with ~~SDS (Short Data Service)~~ short data service messages.

10. (Previously Presented) The method of claim 7 implemented in a wireless terminal equipment.

11. (Currently Amended) A method, comprising:
managing at least ~~dynamic encryption and synchronization applications, and~~
~~distributing the applications based on an established criterion to terminal equipment~~
~~connected to a data communication network~~ one of encryption and synchronization
applications as well as encryption parameters concerning a data communication network; and
distributing the at least one of encryption and synchronization applications as well as the
encryption parameters based on an established criterion to pieces of terminal equipment.